Safety Function: Two Hand Control
Products: 800Z Zero-Force Buttons
GuardLogix® Controller
POINT Guard Safety I/O™ Modules

Safety Rating: PLe, Cat. 4 to EN ISO 13849.1 2008

LISTEN. THINK. SOLVE.®

Allen-Bradley • Rockwell Software

Rockwell Automation

Table of Contents

Introduction	3
Important User Information	3
Safety Function Realization	4
General Safety Information	5
Setup and Wiring	7
Configuration	8
Programming	15
Calculation of the Performance Level	17
Verification and Validation Plan	19
Additional Resources	22

Introduction

This Safety Function application note explains how to wire, configure, and program a Compact GuardLogix® controller and POINT Guard I/O™ module to monitor a two hand run station. Only when the operator places their hands on the buttons, signifying the operator location, can the GuardLogix controller energize the final control device, in this case, a redundant pair of 100S contactors.

This example uses a Compact GuardLogix controller, but is applicable to any GuardLogix controller. This example uses 800Z Zero-Force Touch buttons™, but is applicable to buttons with one (1) N/C dry contact and one (1) N/O dry contact.

The SISTEMA calculations shown later in this document would have to be re-calculated using the actual products.

Important User Information

Solid state equipment has operational characteristics differing from those of electromechanical equipment. Safety Guidelines for the Application, Installation and Maintenance of Solid State Controls (publication **SGI-1.1** available from your local Rockwell Automation® sales office or online at **http://www.rockwellautomation.com/literature**) describes some important differences between solid state equipment and hard-wired electromechanical devices. Because of this difference, and also because of the wide variety of uses for solid state equipment, all persons responsible for applying this equipment must satisfy themselves that each intended application of this equipment is acceptable.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

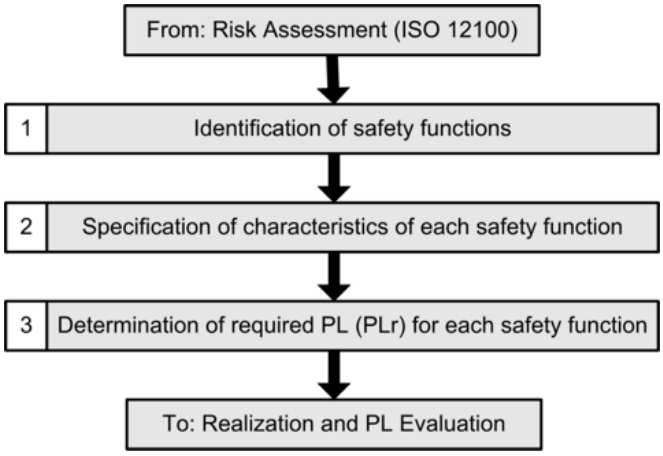
The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Safety Function Realization: Risk Assessment

The required performance level is the result of a risk assessment and refers to the amount of the risk reduction to be carried out by the safety-related parts of the control system. Part of the risk reduction process is to determine the safety functions of the machine. For the purposes of this document the assumed required performance level is Category 4, PLe.


From: Risk Assessment (ISO 12100)
1
Identification of safety functions
2
Specification of characteristics of each safety function
3
Determination of required PL (PLr) for each safety function
To: Realization and PL Evaluation

Two Hand Control Safety Function

The safety function is the removal of power from the hazard when the safety system detects that the operator does not have both hands on the palm buttons.

Safety Function Requirements

Functional Safety is obtained by use of a controlled location of an operator's hands during hazardous motion. Continuous actuation of two pushbuttons is required to enable power to the motor. Upon releasing either of the two pushbuttons, power to the motor will be removed. Faults at the two-hand pushbuttons, wiring terminals or safety controller will be detected before the next safety demand. The safe distance location of the two-hand control station must be established such that the hazardous motion must be stopped before the operator can reach the hazard.

The safety function in this example is capable of connecting and interrupting power to motors rated up to 9A, 600VAC. The safety function will meet the requirements for Category 4, Performance Level "e" (Cat 4, PLe), per ISO 13849-1, and SIL3 per IEC 62061, and control reliable operation per ANSI B11.19.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.

	WARNING: Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.
IMPORTANT	Identifies information that is critical for successful application and understanding of the product.
	ATTENTION: Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.
	SHOCK HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.
	BURN HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.

General Safety Information

Contact Rockwell Automation to find out more about our safety risk assessment services.

IMPORTANT	This application example is for advanced users and assumes that you are trained and experienced in safety system requirements.
	ATTENTION: A risk assessment should be performed to make sure all task and hazard combinations have been identified and addressed. The risk assessment may require additional circuitry to reduce the risk to a tolerable level. Safety circuits must take into consideration safety distance calculations which are not part of the scope of this document.

Functional Safety Description

In this example, if the machine is waiting to cycle, the operator must place both hands on individual palm buttons to energize a pair of redundant safety contactors, enabling machine motion. The palm buttons are each wired to a pair of safety inputs on a Safety Input module (SI1). The safety contactors (K1 & K2) are connected to a pair of safety outputs on a Safety Output module (SO1). The I/O module is connected via CIP Safety over an EtherNet/IP network to the Safety Controller (SC1). The safety code in SC1 monitors the status of the palm buttons using the pre-certified safety instruction 'Two Hand Run Station' (THRSe). When all safety input interlocks are satisfied, no faults are detected, the machine is prepared to cycle, and the palm buttons are pressed, a certified function block called Configurable Redundant Output (CROUT) controls and monitors feedback for a pair of 100S redundant contactors.

Bill of Material

Catalog Number	Description	Quantity
800Z-GL2065	800Z Zero-Force Touch Button with no guard	2
800FM-G611MX10	800F Reset Push Button - Metal, Guarded, Blue, R, Metal Latch Mount, 1 N.O. Contact(S), Standard	1
100S-C09ZJ23C	Bulletin 100S-C - Safety Contactors	2
1768-ENBT	CompactLogix™ EtherNet/IP Bridge Module	1
1768-L43S	Compact GuardLogix Processor, 2.0 MB standard memory, 0.5 MB safety memory	1
1768-PA3	Power Supply, 120/240 VAC Input, 3.5 A @ 24V DC	1
1769-ECR	Right End Cap/Terminator	1
1734-AENT	24V DC Ethernet Adapter	1
1734-TB	Module Base with Removable IEC Screw Terminals	4
1734-IB8S	POINT Guard Safety Input Module	1
1734-OB8S	POINT Guard Safety Output Module	1
1783-US05T	Stratix 2000™ Unmanaged Ethernet Switch	1

Setup and Wiring

For detailed information on installing and wiring, refer to the product manuals listed in the **Additional Resources**.

System Overview

The 1734-IB8S input module monitors the N.C. and N.O. contacts of both 800Z Zero-Force buttons.

Because the Zero-Force buttons uses one N.O. and one N.C. contact, all wiring faults will either be detected either before or at the next demand, so there is no reason to perform pulse testing on the channels.

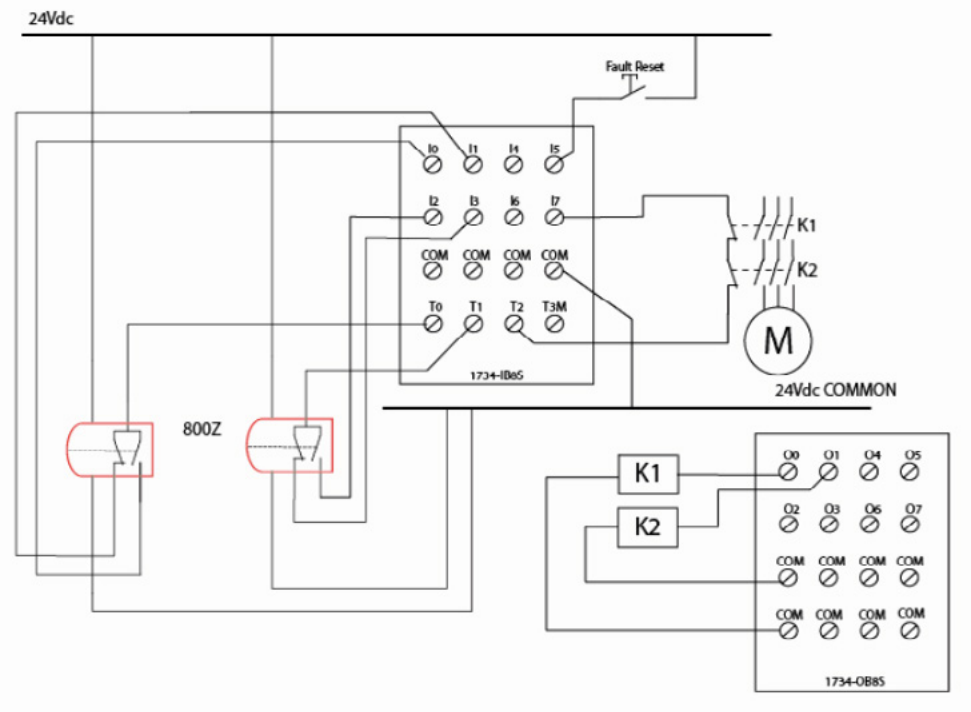
If the inputs remain discrepant for longer than the discrepancy time, then the function blocks in the controller safety task will declare a fault. Only after the fault is cleared and the gate is cycled will the function block reset. Note that in this case, complimentary is the normal state of the contacts; so if equivalent for longer than the discrepancy time, a fault is declared.

The final control device in this case is a pair of 100S safety contactors, K1 and K2. The contactors are controlled by a 1734-OBS safety output module. The contactors are wired in a redundant series configuration. A feedback circuit is wired through the N.O. contacts and back to an input on the 1734-IB8S module to monitor the contactors for proper operation. The contactors cannot restart if the feedback circuit is not in the correct state.

The system has a reset button for resetting faults.

Note that the reset button and the contactor feedback circuit are both wired to the 1734-IB8S module in this example. This is not required for functional safety. These inputs could be wired to a standard input module.

Electrical Schematic



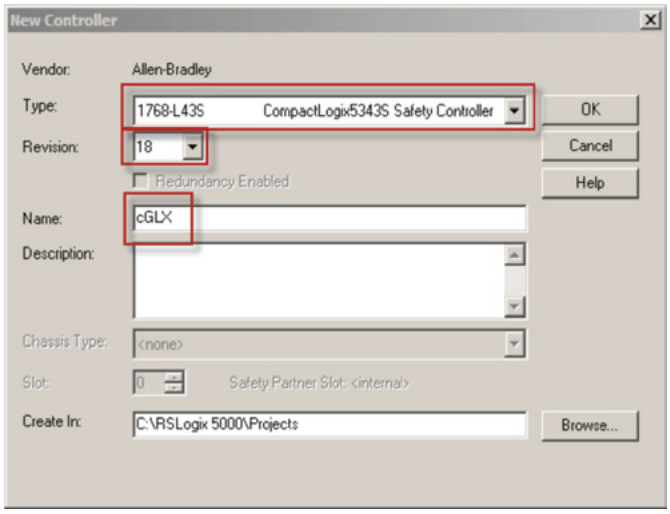
Configuration

The Compact GuardLogix controller is configured by using RSLogix™ 5000 software, version 17 or later. You must create a new project and add the I/O modules. Then, configure the I/O modules for the correct input and output types. A detailed description of each step is beyond the scope of this document. Knowledge of the RSLogix programming environment is assumed.

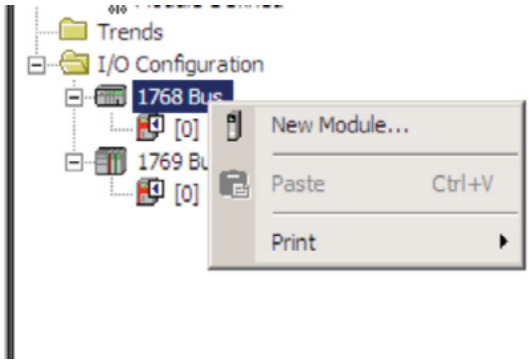
Configure the Controller and Add I/O Modules

Follow these steps.

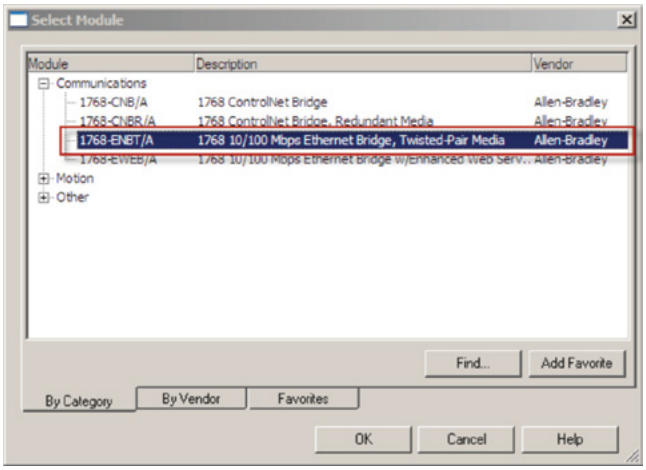
1. In RSLogix 5000 software, create a new project.



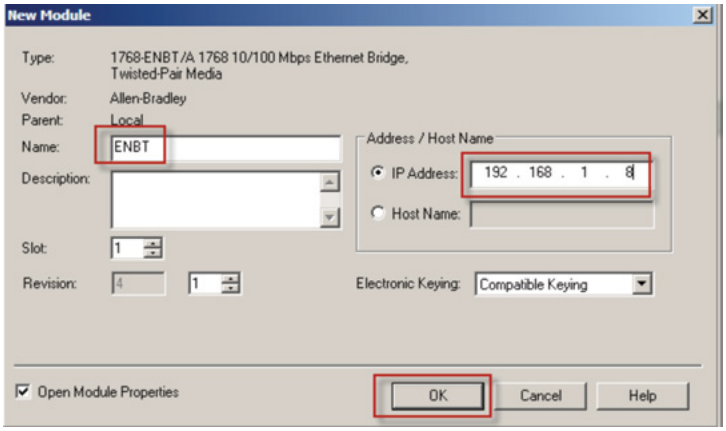
2. In the Controller Organizer, add the 1768-ENBT module to the 1768 Bus.



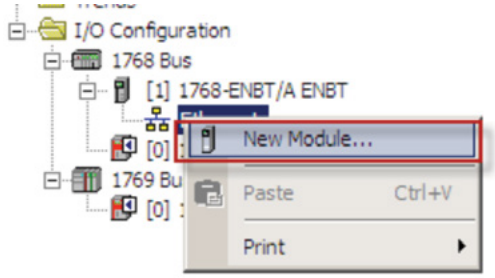
3. Select the 1768-ENBT module and click OK.



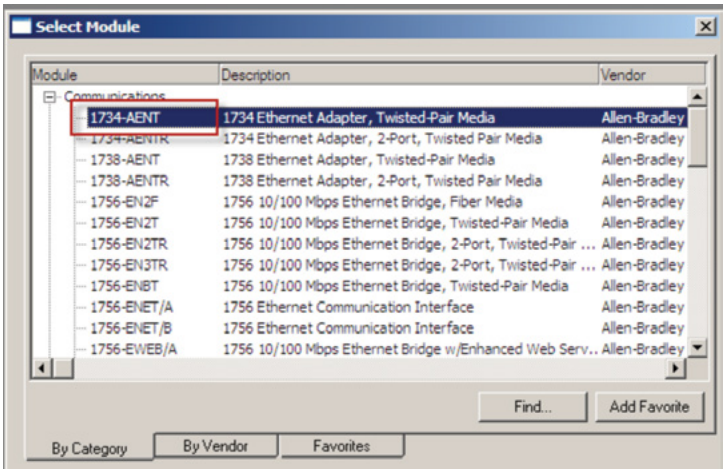
4. Name the module, type its IP address, and click OK.
   We used 192.168.1.8 for this application example. Yours may be different.



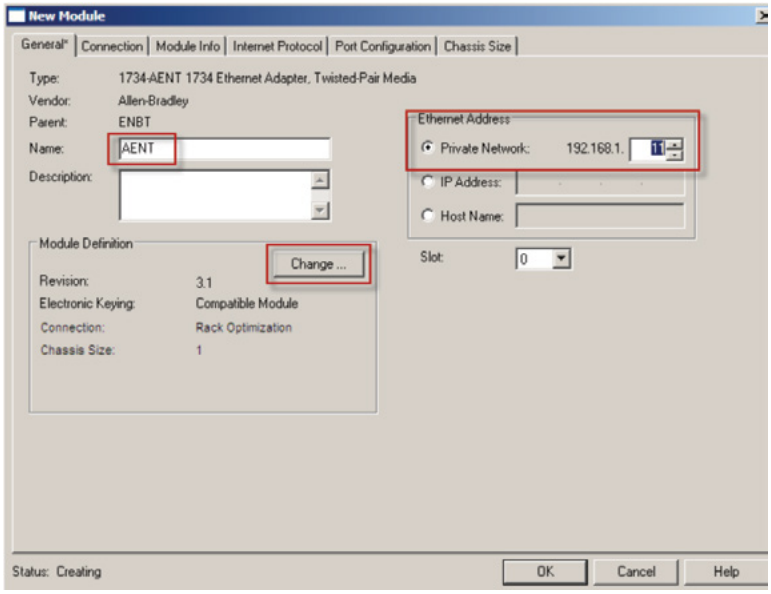
5. Add the 1734-AENT adapter by right-clicking the 1768-ENBT module in the Controller Organizer and choosing New Module.



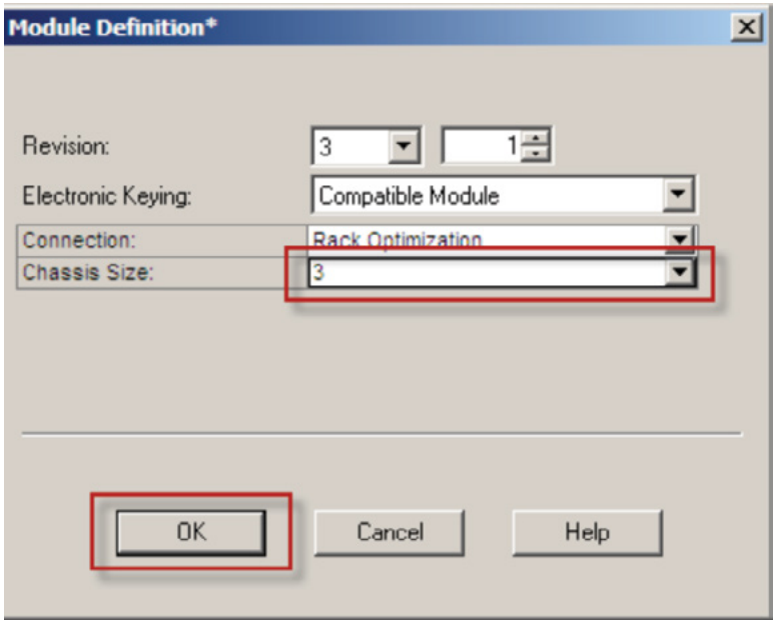
6. Select the 1734-AENT adapter and click OK.



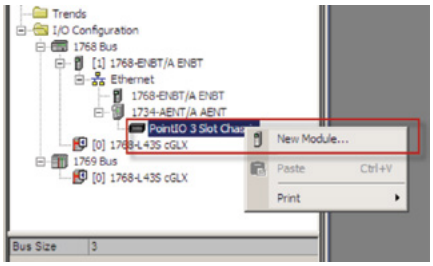
7. Name the module, type its IP address, and click OK.
   We used 192.168.1.11 for this application example. Yours may be different.
8. Click Change.



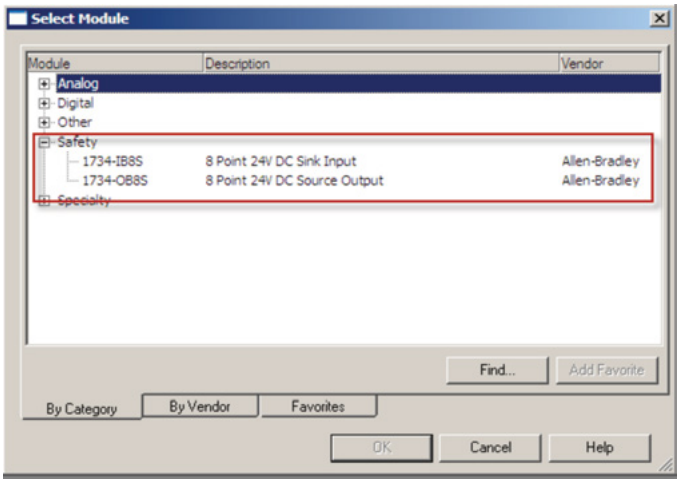
9. Set the Chassis Size as 3 for the 1734-AENT adapter and click OK.
   Chassis size is the number of modules that will be inserted in the chassis. The 1734-AENT adapter is considered to be in slot 0, so for one input and one output module, the chassis size is 3.



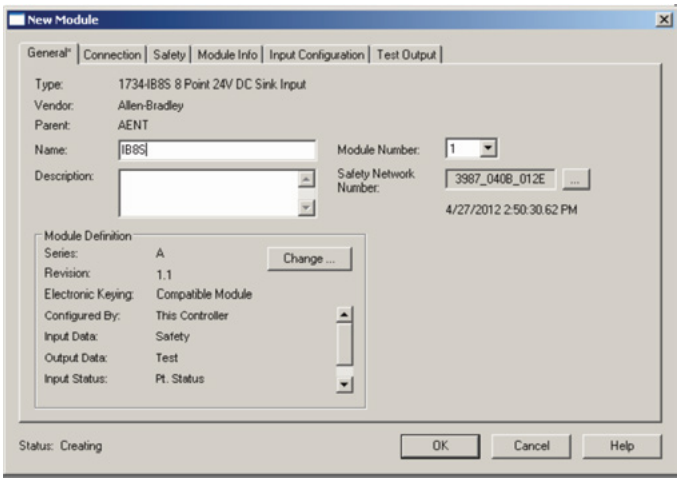
10. In the Controller Organizer, right-click the 1734-AENT adapter and choose New Module.



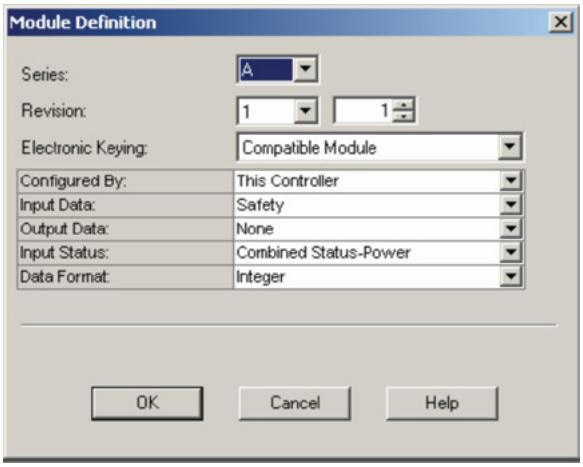
11. Expand Safety, select the 1734-IB8S module, and click OK.



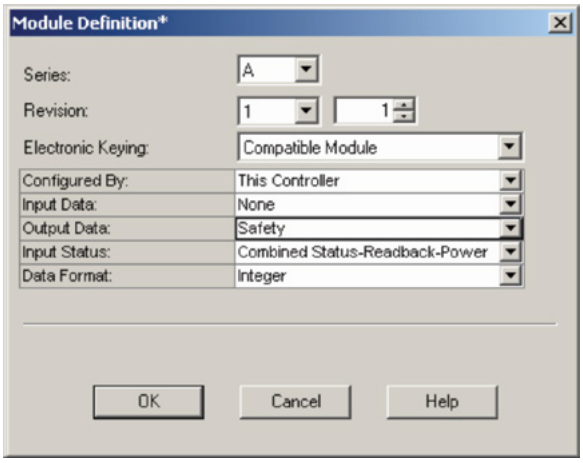
12. In the New Module dialog box, name the device 'IB8S'and click Change.



13. When the Module Definition dialog box opens, change the Output Data to 'None' and verify the Input Status is Combined Status-Power', and click OK. Setting the output data to None means that you cannot use the Test Outputs as standard outputs, and we are not doing that in this example. Note this saves one (1) controller connection because we are only using the input connection.



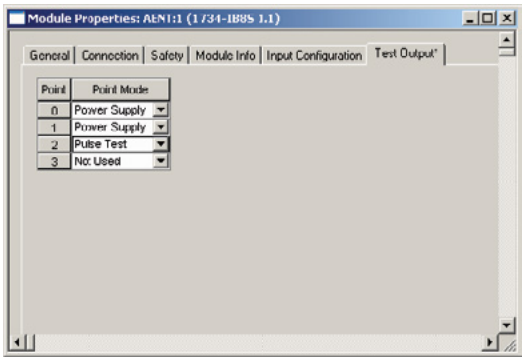
14. Close the Module Properties dialog box by clicking OK.
15. Repeat steps 10-14 to add the 1734-OB8S safety output module. Name the module OB8S. Note this module will be in slot 2, and select 'Combined Status-Readback-Power' for Input Status definition.



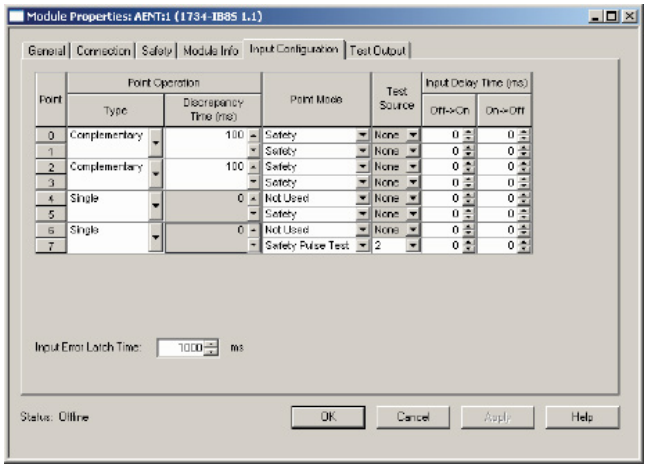
Configure the I/O Modules

Follow these steps to configure the POINT Guard I/O modules.

1. In the Controller Organizer, right-click the 1734-IB8S module and choose Properties.
2. Click Test Output and configure the module as shown. T0 and T1 are being used to source 24Vdc for the 800Z buttons. Note that the 24Vdc could be sourced directly from a power supply. Sourcing from T0 and T1 is not required for functional safety. T2 is being used to pulse test the contactor feedback circuit.

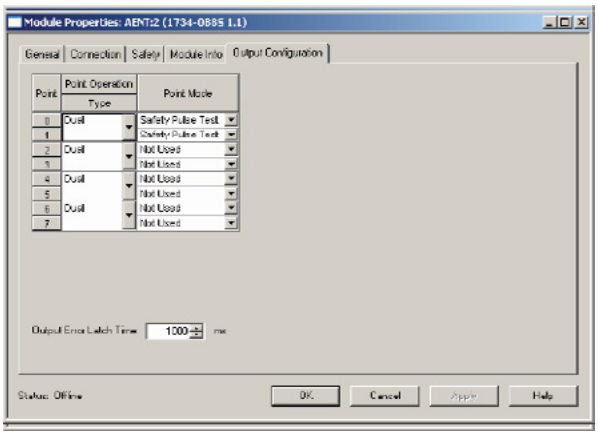


3. Click Input Configuration and configure the module as shown. Inputs 0/1 are the TLS3-GD2 door monitoring contacts. Recall that inputs 0/1 are being sourced from test outputs 0/1. Inputs 2/3 are the lock monitoring contacts. They are also being sourced from test outputs 0/1. Inputs 4/5 are the reset buttons. Input 7 is the contactor monitoring circuit. Recall that input 7 is being sourced from Test Output 2. Note that there really is no difference when an input channel is configured for safety or standard. It is used more for documentation.



4. Click OK.
5. In the Controller Organizer, right-click the 1734-OB8S module and choose Properties.

6. Click Output Configuration and configure the module as shown. The electromechanical coil on the contactor (outputs 0/1) can be pulse tested without reacting to the brief LO pulse.



7. Click OK.

Programming

The Two Hand Run Station (THRSe) instruction monitors dual channel buttons and turns on its output when the buttons are pressed within the discrepancy time, one (1) second in this example. The THRSe has an 'Enable' input that must be HI for the output to turn on. In this example, it represents a 'machine is ready to cycle' tag that is a summation of safety interlocks and standard machine run code. This programming is outside the scope of this document.

Input Status typically represents the channel status of the four (4) input channels. In this example, the 'Combined Input Status' bit goes LO if any of the 8 input channels on the 1734-IB8S module has a fault.

The output (O1) of the THRSe is used to energize the 'outputs enabled' tag that drives the 'Actuate' input of the CROUT. 'Outputs Enabled' will de-energize if the machine cycle completes or the operator removes their hands from the buttons.

The Configurable Redundant Output (CROUT) instruction controls and monitors redundant outputs. Essentially this instruction verifies that feedback follows the safety outputs appropriately. For the negative feedback used in this example; if the outputs are HI, the feedback should be LO and vice versa. In this example, the feedback has 500ms to change to the proper state. Since only a single feedback circuit is being used, the feedback tag is used for both Feedback 1 and 2.

The two (2) output tags from the CROUT instruction are used to drive the contactor outputs on the 1734-OB8S module.

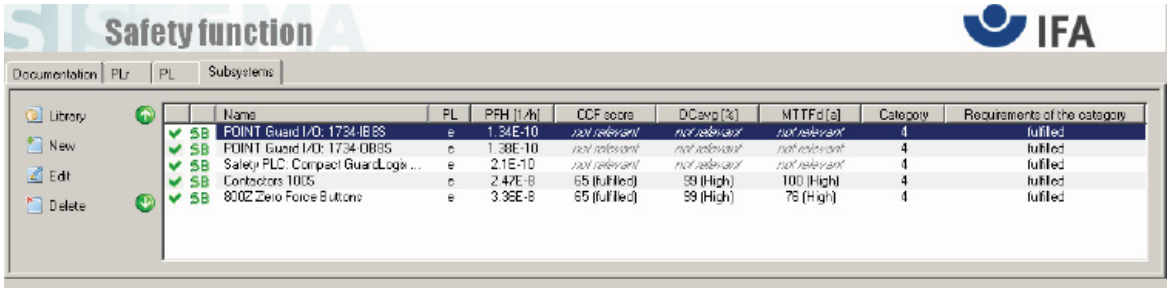
THRSe
Two Hand Run Station Enhanced
THRSe THRS
Discrepancy Time (Msec) 1000
Enable Machine_Ready_to_Cycle
Disconnected disconnected
Right Button Normally Open AENT:1:I.Pt00Data
Right Button Normally Closed AENT:1:I.Pt01Data
Left Button Normally Open AENT:1:I.Pt02Data
Left Button Normally Closed AENT:1:I.Pt03Data
Input Status AENT:1:I.CombinedInputStatus
Reset AENT:1:I.Pt05Data
THRS.O1 Machine_Cycle_Complete safety_contactors.FP
Outputs_Enabled
CROUT
Configurable Redundant Output
CROUT safety_contactors
Feedback Type NEGATIVE
Feedback Reaction Time (Msec) 250
Actuate Outputs_Enabled
Feedback 1 AENT:1:I.Pt07Data
Feedback 2 AENT:1:I.Pt07Data
Input Status AENT:1:I.CombinedInputStatus
Output Status AENT:2:I.CombinedOutputStatus
Reset AENT:1:I.Pt05Data
safety_contactors.O1 safety_contactors.O2
AENT:2:O.Pt00Data
AENT:2:O.Pt01Data
(End)

Calculation of the Performance Level

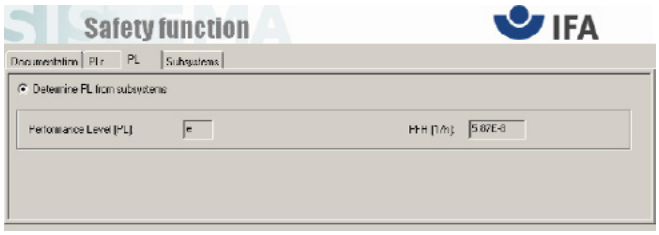
When configured correctly, this Door Monitoring and Locking safety function can achieve a safety rating of PLe, Cat. 4 according to EN ISO 13849.1 2008.

The Functional Safety Specifications of the project call for a Performance Level on PLd (minimum) and a structure of Cat 3 (minimum). A PFHd of less than 1.0 E-06 for the overall safety function is required for PLd.

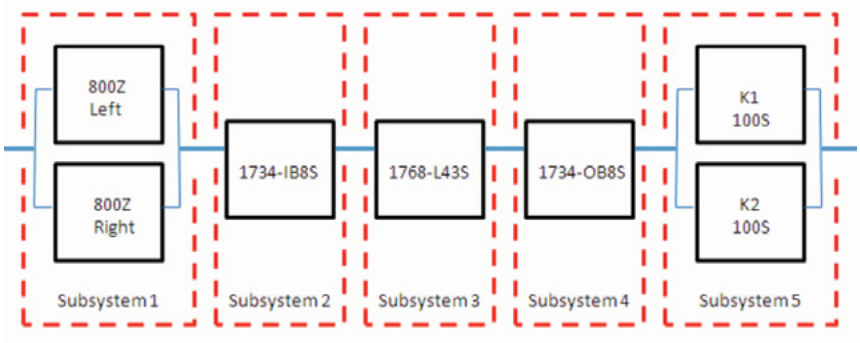
The individual subsystem values are shown below.



The overall safety function value is shown below.



The Two Hand Run Station safety function can be modeled as shown in the following safety related block diagram:



As the Zero-Force Touch Buttons are not electromechanical, the MTTFd is not based on cycles, but time. The MTTFd is 76 years. Contactor calculations are based on 1 operation of the Run Station per minute; therefore 525,600 operations of contactors per year.

The measures against Common Cause Failure (CCF) are quantified using the scoring process outlined in Annex F of ISO 13849-1. For the purposes of the PL calculation, the required score of 65 needed to fulfill the CCF requirement is considered to be met. The complete CCF scoring process must be done when implementing this example.

SB 800Z Zero Force Buttons	
PL	e
PFH [1/h]	3.36E-8
Cat.	4
MTTFd [a]	76 (High)
DCavg [%]	99 (High)
CCF	65 (fulfilled)

SB POINT Guard I/O: 1734-IB8S	
PL	e
PFH [1/h]	1.34E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

SB Safety PLC: Compact GuardLogix 1768	
PL	e
PFH [1/h]	2.1E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

SB POINT Guard I/O: 1734-OB8S	
PL	e
PFH [1/h]	1.38E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

SB Contactors 100S	
PL	e
PFH [1/h]	2.47E-8
Cat.	4
MTTFd [a]	100 (High)
DCavg [%]	99 (High)
CCF	65 (fulfilled)

Verification and Validation Plan

Verification and Validation play an important role in the avoidance of faults throughout the safety system design and development process. ISO/EN 13849-2 sets the requirements for verification and validation. It calls for a documented plan to confirm all the Safety Functional Requirements have been met.

Verification is an analysis of the resulting safety control system. The Performance Level (PL) of the safety control system is calculated to confirm it meets the Required Performance Level (PLr) specified. The SISTEMA software tool is typically utilized to perform the calculations and assist with satisfying the requirements of ISO 13849-1.

Validation is a functional test of the safety control system to demonstrate that it meets the specified requirements of the safety function. The safety control system is tested to confirm all of the safety related outputs respond appropriately to their corresponding safety related inputs. The functional test should include normal operating conditions in addition to potential fault inject of failure modes. A checklist is typically used to document the validation of the safety control system.

Validation of software development is a process in which similar methodologies and techniques that are used in hardware development are deployed. Faults created through poor software development process and procedure are systemic in nature rather than faults associated with hardware which are considered as random.

Prior to validating the GuardLogix Safety System, it is necessary to confirm the safety system and safety application program have been designed in accordance with the GuardLogix System Safety Reference Manual (1756-RM093) and the GuardLogix Application Instruction Safety Reference Manual (1756-RM095).

GuardLogix Two Hand Control Station Function Verification and Validation Checklist			
General Machinery Information			
Machine Name / Model Number			
Machine Serial Number			
Customer Name			
Test Date			
Tester Name(s)			
Schematic Drawing Number			
Controller Name			
Safety Signature ID			
Safety Network Number(s)			
RSLogix5000 Software Version			
Safety Control System Modules	**GuardLogix Modules**		**Firmware Version**
GuardLogix Safety Controller	1768-L43S		
CompactLogix Ethernet Bridge	1768-ENBT		
POINT I/O Ethernet Adapter	1734-AENT		
POINT I/O Input Modules	1734-IB8S		
POINT I/O Output Modules	1734-OB8S		
GuardLogix Safety System Configuration and Wiring Verification			
Test Step	**Verification**	**Pass/Fail**	**Changes/Modifications**
1	Verify the safety system has been designed in accordance with the GuardLogix System Safety Reference Manual 1756-RM093.		
2	Verify the safety application program has been designed in accordance with the GuardLogix Application Instruction Safety Reference Manual 1756-RM095.		
3	Visually inspect the safety system network and I/O is wired as documented in the schematics.		
4	Visually inspect the RSLogix 5000 program to verify that the safety system network and I/O module configuration is configured as documented.		
5	Visually inspect the RSLogix 5000 application program to verify suitable safety certified instructions are utilized. The logic is readable, understandable and testable with the aid of clear comments.		
6	All input devices are qualified by cycling their respective actuators. Monitor the status in the RSLogix 5000 Controller Tags window.		
7	All output devices are qualified by cycling their respective actuators. Monitor the status in the RSLogix 5000 Controller Tags window.		
Normal Operation Verification - The GuardLogix safety system properly responds to all normal Start, Stop, Estop, Lock and Reset Commands			
Test Step	**Verification**	**Pass/Fail**	**Changes/Modifications**
1	Initiate a Start Command by simultaneously pressing both palm buttons. Both contactors should energize for a normal machine run condition. Verify proper machine status indication and safety relay LED indication.		
2	Initiate a Stop Command by simultaneously releasing both palm buttons. Both contactors should de-energize for a normal machine Stop condition. Verify proper machine status indication and safety relay LED indication.		
3	While Stopped, only press the left palm button. The door should remain closed and locked. Both contactors should remain de-energized and open for a normal safe condition. Verify proper machine status indication and RSLogix 5000 safety application program indication. Repeat for right palm button.		
4	Initiate Reset Command. Both contactors should remain de-energized. Verify proper machine status indication and RSLogix 5000 safety application program indication.		

Abnormal Operation Verification - The GuardLogix safety system properly responds to all foreseeable faults with corresponding diagnostics. Two Hand Run Station Tests			
Test Step	**Validation**	**Pass/Fail**	**Changes/Modifications**
1	While Stopped, press the left palm button followed by the right 1 sec. later. Both contactors should remain de-energized and open. Verify proper machine status indication and RSLogix 5000 safety application program indication. Verify unable to reset and restart with fault. Repeat for sequence starting with the right palm button.		
2	While Running, remove the Channel 1 wire from the Safety I/O. Both contactors should de-energize. Verify proper machine status indication and RSLogix 5000 safety application program indication. Verify unable to reset and restart with fault. Repeat for Channel 2.		
3	While Running, short Channel 1 of the Safety I/O to +24VDC. Both contactors should de-energize. Verify proper machine status indication and RSLogix 5000 safety application program indication. Verify unable to reset and restart with fault. Repeat for Channel 2.		
4	While Running, short Channel 1 of the Safety I/O to (-) 0VDC. Both contactors should de-energize. Verify proper machine status indication and RSLogix 5000 safety application program indication. Verify unable to reset and restart with fault. Repeat for Channel 2.		
5	While Running, short Channels 1 & 2 Safety I/O. Both contactors should de-energize. Verify proper machine status indication and RSLogix 5000 safety application program indication. Verify unable to reset and restart with fault.		
GuardLogix Controller and Network Tests			
Test Step	**Validation**	**Pass/Fail**	**Changes/Modifications**
1	While Running, remove the Ethernet network connection between the Safety I/O and the controller. All contactors should de-energize. Verify proper machine status indication and I/O Connection Status in the RSLogix 5000 safety application program.		
2	Restore the Safety I/O module network connection and allow time to reestablish communication. Verify the Connection Status Bit in the RSLogix 5000 safety application program. Repeat for all Safety I/O connections.		
3	While Running, switch the controller out of Run Mode. All contactors should de-energize. Return key switch back to Run Mode, all contactors should remain de-energized. Verify proper machine status indication and RSLogix 5000 safety application program indication.		
Safety Contactor Output Tests			
Test Step	**Validation**	**Pass/Fail**	**Changes/Modifications**
1	Initiate a Start Command. Both contactors should energize for a normal machine run condition. Verify proper machine status indication and RSLogix 5000 safety application program indication.		
2	While Running, remove the contactor feedback from the Safety I/O. All contactors should remain energized. Initiate a Stop command and attempt a Reset command. The system should not Restart or Reset. Verify proper machine status indication and RSLogix 5000 safety application program indication.		
3	While Running, short the contactor feedback to the Safety I/O. All contactors should remain energized. Initiate a Stop command and attempt a Reset command. The system should not Restart or Reset. Verify proper machine status indication and RSLogix 5000 safety application program indication.		

Additional Resources

For more information about the products used in this example refer to these resources.

Resource	Description
Compact GuardLogix Controllers User Manual, Publication 1768-UM002	Provides information on configuring, operating, and maintaining Compact GuardLogix controllers.
POINT Guard I/O Safety Modules Installation and User Manual, Publication 1734-UM013	Provides information on installing, configuring, and operating POINT Guard I/O Modules.
GuardLogix Controller Systems Safety Reference Manual, Publication 1756-RM093	Contains detailed requirements for achieving and maintaining safety ratings with the GuardLogix controller system.
GuardLogix Safety Application Instruction Set Reference Manual, Publication 1756-RM095	Provides detailed information on the GuardLogix Safety Application Instruction Set.
Safety Accelerator Toolkit for GuardLogix Systems Quick Start Guide, Publication IASIMP-QS005	Provides a step-by-step guide to using the design, programming, and diagnostic tools in the Safety Accelerator Toolkit.
Safety Products Catalog	

You can view or download publications at http://www.rockwellautomation.com/literature. To order paper copies of technical documentation, contact your local Allen-Bradley® distributor or Rockwell Automation sales representative.

For More Information on Safety Function Capabilities, visit:

discover.rockwellautomation.com/safety

Rockwell Automation, Allen-Bradley, GuardLogix, RSLogix 5000, CompactLogix, Stratix 2000, and POINT Guard I/O are trademarks of Rockwell Automation, Inc.
Trademarks not belonging to Rockwell Automation are property of their respective companies.

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication SAFETY-AT062B-EN-E – January 2013
Supersedes Publication SAFETY-AT062A-EN-E – October 2012

Copyright ©2013 Rockwell Automation, Inc. All Rights Reserved.